Automated Information Systems
Year 2000
Audit Program

OBJECTIVES

Overall Objective:

Does the Army's Year 2000 (Y2K) Action Plan provide an adequate framework for assuring, specifically in terms of contingency options and costs, that all critical systems will be Y2K compliant by system unique data horizons or mandated timeframes.

Subobjectives:

1. Have Army organizations made adequate progress in identifying their critical systems (IAW the Army's Y2K Action Plan) and in committing appropriate personnel and dollar resources to make cost-effective Y2K compliance fixes?

2. Are testing plans comprehensive and complete? For example, do testing plans identify testing facilities, test site requirements (both technical and financial), test site capabilities and have they been scheduled and are they adequate enough so that all critical Army systems and the systems they interface with are cost-effectively tested and certified as Y2K compliant by system unique date horizons or within mandated timeframes?

3. Have Army organizations developed adequate contingency plans with trigger dates to ensure that timely and cost-effective alternatives are initiated to correct Y2K system failures if planned retirement, replacement, or modification milestones cannot be met?

SCOPE OF REVIEW

The Army Audit Agency will focus its Y2K efforts on the Army's mission critical systems. As of the 14 July 1997 data call, the Army's Y2K database showed 818 Major Army systems, of which 367 systems were reported as "critical." Our focus is on the 367 systems that have been reported as "critical systems" by DA Functional Proponents, Major Commands, Program Executive Offices, and/or Program Mangers.

The Army Audit Agency is taking a phased audit approach. The audit phases, reporting requirements, and timelines are at Annex A. We will validate the Army's progress by critical system as reported by Army organizations in the DA Y2KDB. A breakout of the 367 critical systems by functional area, activity, and functional proponent is at Annex B. The initial systems that we will assess in this phase of the effort is at Annex C.

The Army adopted a five-phase resolution process for tracking the Y2K problem consistent with DOD guidance. The five phases are -

Awareness (31 Dec 95-31 Dec 96)--Make personnel responsible for the system aware of problem

Assessment (31 Mar 96-31 Mar 97)--Scope of Y2K impact is identified. For example:

- 100% inventory of systems is completed and prioritized
- Strategy and plan developed and documented to correct the deficiencies
- Resources identified to fix the problems
- Risk management and contingency strategy/plan developed and documented

Renovation (31 Dec 96-30 Sep 98)--Required system "fixes" are accomplished. "Bridges" required to interface with systems/databases are developed at this time

Validation (31 Mar 97-31 Dec 98)--Systems confirmed as Y2K compliant through assorted testing and certification

Implementation (30 Jun 97-31 Dec 98)--Systems are fully operational after being certified

About 60% of the 367 critical systems reported by Army organizations were in the assessment phase after the 14 July 1997 Army data call. Audit work that will be performed by various audit sites will focus on the overall reasonableness of the management and execution of the organizations process for fixing its Y2K problems. You will need to use the timelines shown above throughout your assessment.

DEFINTIONS

Mission Critical Systems: An Army system, that when its capabilities are degraded, the organization realizes a resulting loss of its core capabilities.

System Unique Date Horizons: A date that a critical system uses that will cause a Year 2000 problem before the Year 2000 or before the Army's 31 December 1998 mandated implementation/certification date. For example, systems that do projections now for events that occur during or after the Year 2000.

Additional Definitions: Additional definitions that you must become familiar with are contained in the 22 Sep 1997 -- LTG Campbell, DISC4, CIO, SUBJECT: Data Call in Support of U.S. Army Systems Year 2000 Database.

BACKGROUND

The Army's overall management philosophy for the Year 2000 problem is centralized management and decentralized execution. The magnitude of this problem coupled with the Army's management philosophy leads to a potential risk that some critical systems could fail due to the Year 2000 problem, thereby causing some organizations to loose their core business capabilities.

There is a potential serious disruption to critical government functions and services as a result of the upcoming change of century. The Y2K computing problem has received a great deal of attention from Congress, U. S. Office of Management and Budget, U. S. General Accounting Office, and the Department of Defense Inspector General.

For the past several decades, systems have typically used two digits to represent the year, such as "96" for 1996, in order to converse electronic data storage and reduce operating costs. In this format, however, the year 2000 is indistinguishable from 1900 because both years are represented as "00." Therefore, if this problem isn't modified, computer systems and/or applications that use dates or perform data/time sensitive calculations may generate incorrect results beyond the year 1999.

Experts envision that correcting this problem will be labor-intensive and time-consuming, and must be done while systems continue to operate. Many of the federal agencies computer systems were originally designed and developed over 20 years ago, are poorly documented, and use a variety of computer languages--many of which are obsolete or old. Systems consist of tens of hundreds of computer programs, each with thousands, tens of thousands, or even millions of lines of code that must be examined for date format problems. In addition, the systems have numerous components that are possibly affected by the date problem--hardware, operating systems, communications applications, and database software.

Whether agencies, in our case the Army, succeed or fail, largely depends on, and is influenced by the quality of executive leadership and program management. The challenge in achieving Y2K compliance is not a *technical* problem, but rather a *management* problem. It is important for top management to be aware of the importance of this undertaking, and to communicate this urgency to all agency personnel. Estimates for fixing Army's Y2K problems is over $500 million.

DA GUIDANCE

Key Memorandums:

18 Feb 97	- LTG Guenther, DISC4, CIO, subject: Request for Assistance for the Army's Y2K Action Plan
6 Mar 97	- Memorandum of Understanding (MOU) between Director of Information Management, DISC4 and Deputy Auditor General for Financial Audits, USAAA
31 Mar 97	- Togo West (Secretary of the Army) / General Reimer (Chief of Staff), subject: Year 2000 Fixes -- Top Priority
2 Jun 97	- LTG Guenther, DISC4, CIO, subject: USAAA Y2K Audit Support
12 Jun 97	- LTG Guenther, DISC4, CIO, subject: Use of Year 2000 (Y2K) Compliance Checklist
22 Sep 97	- LTG Campbell, DISC4, CIO, subject: Data Call in Support of U. S. Army Systems Year 2000 Database

DA Action Plan:

U. S. Army Project Change of Century, Action Plan, Revision I, 4 October 96. The plan provides the Army's corporate strategy and management approach for addressing the Y2K problem, as well as the framework and guidance for Army organizations to work with. The plan identifies responsibilities, reporting requirements, and synchronizes ongoing and planned Y2K efforts.

Federal Information Processing Standard (FIPS):

There are three FIPS that may provide guidelines for assessing the reasonableness in the following areas of review:

(i) FIPS #65-Risk Analyses/Assessments
(ii) FIPS #87-Contingency Planning
(iii) FIPS #101-Lifecycle Validation, Verification and Testing of Computer Software

REPORTING REQUIREMENTS

Audit-Control-Point (ACP): The ACP will -

- Issue Memorandum Reports or Action Memorandums with suggested actions that are dual addressed to the Army's Director of Information Management and the Commander or Director of the Organizations audited.

- Brief DISC4 Executives quarterly or more frequently based on the audit results and significance of issues identified by the audit sites during their field work.

Audit Sites: Audit sites will -

- Provide audit results to the Y2K ACP in memorandum report or action memorandum report format. Audit sites will also ensure that significant issues that will adversely affect an organizations ability to become Y2K compliant are immediately addressed to the ACP for elevation to the DISC4 and other appropriate DA, DOD, and Federal Government Organizations.

- Issue Memorandum Reports or Action Memorandums with suggested actions that are dual addressed to the Army's Director of Information Management and the Commander or Director of the Organizations audited.

- Obtain all essential Year 2000 documentation to support the audit work done. Work papers will be provided to the ACP upon completion of reviewing the system(s) for centralized storage. This will ensure that all supporting documentation is maintained at a centralized location should oversight organizations request work papers and supporting documentation for review.

AUDIT POINTS OF CONTACT

Name	Phone Numbers	E-Mail
Pat Fizgerald, Program Director	(703) 681-9585 (DSN) 761-9585	Fitzgerp@aaa.army.mil
Dan Lisewski, Audit Manager	(703) 428-0816 (DSN) 328-0816	Lisewskd@aaa.army.mil
Tim Winnette, Auditor-in-Charge	(703) 275-6018 (DSN) 235-6018	Winnettet@aaa.army.mil

**During this review, if any documents are needed for any of the audit steps, specifically for subobjectives 1 and 3, please contact the following ACP staff members for those documents:

- Subobjective 1 - Ruth Ann Richardson (703) 275-9640 or DSN 235-9640
- Subobjective 3 - Tom Hufford (703) 275-6090 or DSN 235-6090

Audit sites will mail audit work papers, supporting documentation, and their reports to the following address:

U. S. Army Audit Agency
Fort Belvoir Field Office
ATTN: Dan Lisewski/Tim Winnette
8850 Richmond Highway, Suite 200
Alexandria, VA 22309

AUDIT GUIDE/STEPS

NOTE - The audit guide/steps coincides with the four performance measures that we plan to update HQDA managers on a quarterly basis.

4 Performance Measures: We will monitor Army's progress quarterly by these measures -

1. **Status of Critical Systems -** Using the DA Y2K database, on a quarterly basis, we will compare where the Army systems are in regards to the Army's established timeline.

2. **Strategic Plans -** Measure reasonableness of the plans (e.g., testing, timeframes, interface agreements, resources, fielding and expertise).

3. **Replacement Systems -** Establish baseline of replacement systems, and monitor the progress for planned and actual fielding of those replacement systems to ensure they are fielded on time.

4. **Contingency Plans -** Evaluate the reasonableness of contingency plans established for all the critical systems, and what are the resource and operational impact if those systems aren't going to be Y2K compliant by Year 2000.

PRELIMINARY SITE WORK PREPARATION

Provide ACP and field office personnel performing the "Site Work" the following (if necessary) -

- DA IPR Charts briefed by respective Y2K POCs, if available (good background)

- Current Army Y2K database downloads of key information pertaining to the individual systems being reviewed, and downloads for all systems if site work is initiated at the Army Y2K POC (e.g., FP, MACOM, or PEO levels). Key data elements to be downloaded follow --

    - System_Acronym
    - System_Name
    - Weapon_System
    - FP_Acronym
    - PM_Organization
    - Organization_Level
    - PM_POC_Last_Name
    - PM_POC_COM_Phone
    - Y2K_Compliance_Strategy
    - Y2K_Compliance_Phase
    - Current_Phase_Est_Completion_Date
    - Funding_Fix_Identified
    - Est_HD_Y2K_Compliance_Cost
    - Est_HD_Budget_Shortfall
    - Est_SW_Y2K_Compliance_Cost
    - Est_SW_Budget_Shortfall
    - Contingency_Plan
    - Risk Assessment Completion
    - Replacement_Sys_Name
    - Replacement_Sys_Planned Date
    - Replacement_Sys_Actual_Date
    - Actual_Syst_Term_Date
    - Y2K_Compl_Ck
    - Y2K_Certification
    - Interface Information - (DIST and NON_DIST Interface information)

        - System Acronym and Name
        - Provides Data to Main System; and, is input Y2K Compliant
        - Receives Data from Main System; and, is output Y2K Compliant

Assist site work auditors with any discrepancies and/or issues that arise, such as information accuracy and/or policy/guidance issues, during the review of critical systems at that activity.

SUBOBJECTIVE 1: Have Army organizations made adequate progress in identifying their critical systems (IAW the Army's Y2K Action Plan) and in committing appropriate personnel and dollar resources to make cost-effective Y2K compliance fixes? (Relates to Performance Measure 1: Status of Critical Systems).

AUDIT CONTROL POINT:

AUDIT STEPS:

1. Determine the status of Army critical systems in relation to the Army timeline for each quarterly data call. Specifically -

    - Prepare a bar chart graph for the systems, and compare the number in each phase vs. where the system should be IAW the Army timeline.

    - For all the systems, perform a query against the DA Y2KDB data element - "current_phase_est_completion_date." Specifically, how many systems in -

        - Assessment don't have dates, or have dates that look unreasonable (i.e., late assessment estimated completion date when comparing with Implementation Phase start date) - thus, draw possible conclusion of "high risk area"

        - Renovation, Validation or Implementation have unreasonable estimated completion dates based on the Army timelines (i.e., estimated completion dates go beyond next phase or into the last year - Implementation phase, ear-marked for fixing possible problems, thus, possible conclusion - high risk area"

    - How many critical systems don't identify a Y2K_Compliance_Strategy, thus, possible conclusion of "high risk area"

2. For all mission critical Army systems as reported in the DA Y2KDB, determine what specific organization is responsible for performing the Y2K fix. This breakout will be necessary for us to evaluate whether other systems that we don't test in detail can reasonably be expected to be Y2K compliant based on our assessment of the management structure and processes that are evaluated.

AUDIT SITES:

Purpose of the audit work is to verify the accuracy of what the organization reports to DA and the actual status of their Y2K system fixes. If you discover major discrepancies between what's reported and the actual status, it's very critical to determine what management breakdown(s) caused this to happen and what needs to be done to correct

the problem(s). You will also use this baseline to perform the various analyses contained in other parts of this audit guide.

Using the download of the critical systems from the DA Y2KDB, perform the following audit step. If you are performing work at the Functional Proponent, Program Executive Officer, or Major Command Levels, the Y2K Point of Contact (POC) should have oversight of all the systems from the download. If you are performing work at the Program Manager Level, the POC may only have information related to that specific system. Contact the Audit Control Point if you have any questions.

AUDIT STEPS:

1. Determine whether the information contained in the download (each data element) is accurately reflected in the Army Y2KDB. If there are inaccuracies, determine why and what management procedures or processes need to be established or fixed. Also, provide the ACP with the correct information validated by this step. The focus of this work is to establish a baseline for a specific system or number of systems depending on where you are performing the audit work.

2. If your analysis shows that mission critical system(s) have fallen 2 months or more behind the Army's Year 2000 timeline schedule - any system still in the Assessment Phase is behind schedule by 2 months or more - determine if management has complied with the mandatory Congressional and OMB reporting requirements. (See the DISC4 memorandum, SUBJECT: Data Call In Support of the US Army Systems Year 2000 Database that we provided you with this audit guide). If management has complied with this requirement, obtain a copy of the report and evaluate it for reasonableness. If Management hasn't complied with this requirement, determine why, and advise them of the requirement and notify the ACP.

SUBOBJECTIVE 2: Are testing plans comprehensive and complete? For example, do testing plans identify testing facilities, test site requirements (both technical and financial), test site capabilities and have they been scheduled and are they adequate enough so that all critical Army systems and the systems they interface with are cost-effectively tested and certified as Y2K compliant by system unique date horizons or within mandated timeframes? (Relates to Performance Measure 2: Strategic Plan)

AUDIT CONTROL POINT:

AUDIT STEP:

1. The ACP will apply the AUDIT SITE steps when reviewing selected systems in detail. The ACP will also consolidate and analyze the work done by audit sites and summarize the work and report as required.

AUDIT SITES:

The purpose of this audit work is to use the Army Y2KDB download that you baselined in Subobjective 1 and to evaluate whether what is being reported reasonably represents the organization's true Y2K status of critical system fixes. In performing this analysis you are trying to verify whether the overall plan will ensure that all critical systems are Y2K compliant within established Army timelines or system unique date horizons. This is **THE MOST CRITICAL ANAYSIS** because it will validate whether what is being reported is the actual status of that critical system and whether the system(s) will be tested, certified compliant, and fielded far enough in advance to make sure that all interfaces and unknown glitches are identified and corrected prior to Year 2000. Your primary focus will be the system or systems that are contained in the Initial Systems to Assess for your location at Annex C. Our goal is to try to extend the results of your detailed system review to other systems the organization has responsibility for fixing, testing, certifying, and fielding.

PROJECT MANAGEMENT PLAN. Depending on whether you are looking at a specific system (Program Manager Level) or a number of systems (DA Functional, Program Executive Officer, or Major Command Level) there should be an overall management plan for a specific system or group of systems. This plan should identify all information technology components and interfaces with other system(s) for the possibility of having Y2K problems. This risk analysis/assessment includes the technical environment on which the system operates, communication devices the system uses, and the application of software itself. This assessment should include the development of a strategy and plan to fix, test, certify, and field critical systems and all related interfaces by the Year 2000 problem.

AUDIT STEPS:

1. Obtain an understanding of the how the Year 2000 crisis is being managed at your audit location. In doing this, document the management structure and processes that are in place. Because we can't evaluate every system, this understanding of how the crisis is being managed by the organization at your audit site is critical for identifying potential systemic management breakdowns that could cause systems that we don't review to fail because of a Year 200 compliance failure.

2. Obtain the Organization's Year 2000 Management Plan for the system or systems at the audit sites. Determine whether a risk analysis/assessment was done to quantify the number of critical systems and related interfaces affected by the Year 2000. This assessment should include identifying (i) the type of fix required (replace, retire, or renovate - procedural code change, sliding window, or bridge), (ii) testing requirements (expertise, facilities, equipment, personnel, funds, and scheduling), (iii) how the system(s) and related interfaces will be certified Y2K compliant as a whole, (iv) when the last unit needs to be fielded, and (v) contingencies for offsetting risks that could affect making critical systems Year 2000 compliant as planned by the organization.

a) If an assessment was done, obtain a copy and determine if it contains elements (i) through (v) above, and evaluate the reasonableness of the assessment and whether it complements what's being reported in the Army Y2KDB.

b) If an assessment wasn't done, determine why not, and how this affects the validity of the Army Y2KDB and the overall Year 2000 status of the critical system(s). If a risk assessment wasn't done and the system(s) are in the renovation, validation, or implementation phases, determine how systems reached this stage of the Y2K resolution process.

3. For the system or systems that you are reviewing in detail, perform the following tests and analyses:

a) If the organization at your site is responsible for system development and maintenance:

i) Determine if all nonessential system sustainment requirements and enhancements have been postponed and that Y2K fixes, testing, and certification have been given top priority and are fully funded. If all nonessential system sustainment requirements and enhancements have not been postponed and Y2K fixes have not been prioritized and funded, determine why and notify the ACP.

ii) Determine if a Configuration Control Board (CCB) has been able to prioritize how funds and personnel will be used to perform Year 2000 fixes before other system enhancements and upgrades. If a CCB hasn't been held and there are resource problems that will adversely impact systems from becoming Y2K compliant, notify the ACP immediately.

b) Determine how far along the organization is in completing its Y2K fixes, to include all systems that interface with the system or systems you're reviewing. Determine if they are ahead or behind schedule. If they are behind schedule, determine why and how this will affect their testing, certification, and fielding schedules. Also, verify whether the status agrees with what has been reported in the Army Y2KDB.

c) Determine if interface agreements or Memorandum of Understanding/ Agreement have been established, signed, and are currently in place for ALL interfacing systems. If agreements are in place, obtain copies and do a quick analysis to determine if all schedules coincide. If schedules don't coincide, determine the impact on established fix, test, and fielding schedules. If agreements aren't in place, determine why they aren't and when they will be in place. Evaluate the impact this will have on established fix, test, and fielding schedules.

d) Determine how the organization will test whether critical system(s) are Y2K compliant. Will this be done in-house or by contractor? Do the testing activities have sufficient resources (facilities, equipment, personnel, expertise, and funds) to accomplish the Y2K testing workload? Have test schedules been prepared and coordinated with the government or contractor activities that will perform the Y2K compliance testing? Do these test schedules take into consideration test facility workload necessary to test the system(s) and all interfacing systems as a whole? Evaluate whether testing activities can accomplish all testing requirements within established schedules.

e) Determine how the organization will certify whether its critical system(s) have been fixed, tested, and certified Y2K compliant. Evaluate whether the procedures and process are reasonable.

f) Determine if the organization has certified any of its critical systems as being Y2K compliant. Determine if the mandatory certification checklist was used and the proper approving officials signed off on the certification checklist to include all interfacing systems. Within reason, evaluate whether these systems are in fact Y2K compliant. If not, immediately notify command and the ACP.

SUBOBJECTIVE 3: Have Army organizations developed adequate contingency plans with trigger dates to ensure that timely and cost-effective alternatives are initiated to correct Y2K system failures if planned retirement, placement, or modification milestones cannot be met? (Relates to Performance Measure 3 & 4: Replacement Systems and Contingency Plans).

The purpose of this audit work is twofold. The Audit Control Point will monitor on a quarterly basis the number of critical systems that haven't reported a contingency plan. The scope of this work will include (i) critical systems that will undergo a Y2K fix, (ii) systems that will replace a system, and (iii) systems that are being replaced. Audit sites will assess the reasonableness of contingency plans for the system(s) that they review in detail - e.g., (i) critical systems that will undergo a Y2K fix, (ii) systems that will replace a system, and (iii) systems that are being replaced. If your assessment of a system(s) overall status indicates that schedules for fixing a system or fielding a replacement system won't be done in time, then the activity will need to take action to implement their contingency plan, or develop a contingency plan if one doesn't already exist. In any event, if a contingency plan doesn't exist, the activity must develop one, or have a reasonable and viable alternative course of action. Site audit work will be used to validate contingency plan information that's been reported in the DA Y2KDB.

AUDIT CONTROL POINT:

AUDIT STEPS:

1. Download the following key data elements for replacement system, and any other that you (the ACP) feel are essential for a complete analysis, and analyze! Forward downloads to site auditors that are reviewing replacement systems:

    - System_Acronym
    - System_Name
    - Y2K_Compliance_Strategy (i.e., shows whether or not the system is going to be reported)
    - Replacement_Sys_Name
    - Replacement_Sys_Planned_Date
    - Replacement_Sys_Actual_Date
    - Actual_Syst_Term_Date
    - Funding_Fix_Identified
    - Risk_Assessment_Completed
    - Contingency_Plan

For those audit sites that aren't reviewing replacement systems, please go to the AUDIT SITE guide and execute only audit step 1.

2. Determine quarterly, based on analysis of Army Y2KDB, the number of critical systems that don't have contingency plans. Of the total number of critical systems requiring contingency plans, determine the number of systems that are being replaced and identify whether or not the timelines seem "reasonable" and whether contingency plans are also in place for those systems that are being replaced by the replacement system(s). (Are any of the replacement systems DOD systems - track the status as well).

3. Determine whether the Army Y2KDB accurately reflects the true status of whether or not contingency plans were prepared and are reasonable for the system(s). Using scope identified in above audit step, and using feedback from site work -

    - Do the systems have contingency plans or not. This will show, of total scope, what percentage actually have a plan in place as we progress through the audit.

    - Do the systems have contingency plans in place that are "reasonable!" This will show of the number in place, what percentage of the plans are actually "reasonable."

AUDIT SITES:

AUDIT STEPS:

1. Obtain the contingency plans for the system(s) you are reviewing. Determine what backup plans the organization has if their critical system fix, test, certification, and fielding schedules can't be met, thereby causing a Y2K critical system failure. Based on the results of the above audit steps, evaluate whether the organization needs to either develop or implement their contingency plan(s) or alternative course of action to prevent a critical system Y2K failure.

2. Determine, in addition to your review of whether or not the system(s) contingency plan(s) were reasonable, whether the system(s) being replaced have contingency plan(s), and -

    - If so, what is the resource impact of ensuring the system(s) being replaced are Y2K compliant.

    - If not, why not.